

ABSTRACT:

Communication information transmitted in the broadband communication system may be in a packet format and secured using encryption techniques, for example encryption software, including a means for providing an initial security key and updated security keys to the various pieces of communication equipment located throughout the broadband communication system. When communication equipment, for example a gateway, is first registered with, for example, an IP central station, the IP central station assigns an initial encryption key to the gateway that is assigned and retained by a server, for example a call manager (CM) server, and the gateway (e.g., broadband residential gateway (BRG)). This initial encryption key may be used to establish a secure two way communication between two pieces of communication equipment as an originating point communication equipment (OPCE) and a terminating point communication equipment (TPCE), for example, the BRG (OPCE) and the CM (TPCE), the BRG (OPCE), BRG1, and another BRG (TPCE), BRG2, or the BRG and a gateway for interfacing with another communication system (e.g. VG). Whenever a user first activates a secure communication feature before or during a communication session, the origination point communication equipment (e.g., BRG1) will not send the terminating point communication equipment (e.g., BRG2) a packet including a private key which may be the BRG's initial encryption key. Subsequently the two pieces of communication equipment will encrypt and decrypt communication packets to one another using the private key. The secured encrypted packets may be part of one or more legs in, for example, a conference call, a teleconference, or a multimedia session. The encryption key may be repeatedly updated and changed at various time intervals. The repeated updates may be at periodic (e.g., daily) or at random time intervals. Updates of the encryption key may occur when the secure call feature is active or inactive. For additional security the system may assign a unique randomly generated encryption key to each packet during the communication session and provide each new key to the communication equipment (e.g., BRG) in each prior information packet transmission. A secure call feature may be activated and deactivated by the user at anytime before or

~~during (i.e., real time activation) an existing communication session. The secure call feature may be used to secure one type of media using encryption while not securing other types of media in a multimedia communication session. Alternatively, different media types, for example audio, text, and multimedia audio and video, may be secured at different levels of security using for example different encryption types or algorithms (e.g., DES, PGP, RSA, etc.). A server, for example a call manager (CM), may coordinate a secure communication between two pieces of communication equipment by translating between two different encryption algorithms in two separate legs of a communication session (e.g., a telephone call). Alternatively, the server may send encryption algorithms to a piece of communication equipment so that the various pieces of communication equipment are using the same algorithm. Control of the secure communication may be transferred from, for example an originating gateway to a terminating gateway. In this case the encryption of a secure communication session may begin by using the originating gateway's key but then start using the terminating gateway's key. The on net communications, for example telephone calls, within the broadband communication system may be encrypted but the on net to off net communications for example telephone calls including PSTN portion, may be partially encrypted. Once the communication enters for example the PSTN, it has only that security provided by the traditional wireline PSTN.~~